REMARKS

The Examiner has finally rejected Claims 1, 13, 25, 30-31, and 37 as anticipated under 35 USC 102 by Vainio; has rejected Claims 2-3, 14-15 and 26-27 under 35 USC 103(a) as being unpatentable over Vainio in view of Kuwamoto; has rejected Claims 4, 6-8, 10, 12, 16, 18-20, 22, 24, 28, 32, 34, 39 and 41 under 35 USC 103(a) as being unpatentable over Vainio in view of Schneier; has rejected Claims 9, 11, 21, 23, 33, 35, 38 and 40 under 35 USC 103(a) as being unpatentable over Vainio in view of Schneier and further in view of Lin; and has rejected Claims 1-3, 8, 13-15, 20, and 25-27 under 35 USC 103(a) as being unpatentable over Vainio in view of Hind.

Applicants respectfully disagree with the Examiner's conclusions with regard to the teachings of the Vainio reference. The Vainio reference teaches security measures for Bluetooth communications. Under the Vainio method, a "verifier" device sends a random number to a claimant device, whereupon the claimant device applies a function to the random number to generate a "SRES" response which is

sent to the verifier. At the verifier device, the received SRES is compared to a locally-calculated SRES'.

Applicants respectfully assert that the Vainio reference does not anticipate or obviate the invention as now claimed, alone or in combination with any of the additionally-cited art. First, the Vainio reference does not teach that two send/receive devices generate verification data and send that data to their respective output devices, after which the data are compared at both of the send/receive device. Rather, Vainio requires that one device act as the verifier, to send the random number, receive the SRES, calculate SRES', and perform the verification. Further, Vainio does not teach or suggest that a plurality of verification data values be generated and compared for mutual matches, as is claimed. While the Examiner seeks to analogize successive iterations of Vainio interactions to the claimed invention, Applicants respectfully assert that the generation of verification data by more than one user device is neither taught nor suggested (independent Claims 1, 13, 25, and 30-41, as well as the claims which depend respectively therefrom). The Examiner has stated, in the **Response to Arguments** section of the Office Action, at paragraph 5, the Examiner indicates that

the arguments presented by Applicants do not match the claim language. By this amendment, Applicants amend the language of the independent claims to expressly recite means and steps for comparing the first and second verification data at each of the send/receive devices and that both devices perform the comparison. Applicants maintain that the Vainio reference does not teach or suggest the claim language.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Anticipation under 35 USC 102 is established only when a single prior art reference discloses each and every element of a claimed invention. See: In re Schreiber, 128 F. 3d 1473, 1477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997); In re Paulsen, 30 F. 3d 1475, 1478-1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994); In re Spada, 911 F. 2d 705, 708, 15 USPQ2d 1655, 1657 (Fed. Cir. 1990) and RCA Corp. v. Applied Digital Data Sys., Inc., 730 F. 2d 1440, 1444, 221 USPQ 385, 388 (Fed. Cir. 1984). Since the Vainio reference does not teach steps or means as claimed, it cannot be maintained that Vainio anticipates the invention as set forth in the independent claims, Claims 1, 13, 25, 30-31 and 37.

The Examiner has rejected Claims 2-3, 14-15 and 26-27 under 35 USC 103(a) as being unpatentable over Vainio in view of Kuwamoto. The newly-cited Kuwamoto reference is cited for teaching visual and auditory verification data at a card reading terminal. Applicants acknowledge that Kuwamoto teaches that both a light and a buzzer may be incorporated into a card reader to alert a user to communication conditions. However, addition of a light and buzzer to the Vainio devices would not result in the invention as claimed, since neither Vainio nor Kuwamoto teaches or suggests more than one device generating verification data, placing the verification data in first and second verification data output sections, and comparing the verification data. For a determination of obviousness, the prior art must teach or suggest all of the claim limitations. "All words in a claim must be considered in judging the patentability of that claim against the prior art" (In re Wilson, 424 F. 2d 1382, 1385, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970). If the cited references fail to teach each and every one of the claim limitations, a *prima facie* case of obviousness has not been established by the Examiner. Since neither Vainio nor Kuwamoto teaches the

claimed limitations, a *prima facie* case of obviousness has not been established.

The Examiner has rejected Claims 4, 6-8, 10, 12, 16, 18-20, 22, 24, 28, 32, 34, 39 and 41 under 35 USC 103(a) as being unpatentable over Vainio in view of Schneier as unpatentable over Vainio in view of Schneier. As per Claims 4, 6-7, 16 and 18-19, the Examiner acknowledges that "Vainio does not teach that the first generation algorithm comprises a serial sequence of operators" as claimed, and cites Schneier as disclosing a serial sequence of operators. While Schneier does show hash functions, Applicants respectfully assert that Schneier does not teach or suggest a serial sequence of operators that are composed of more than one operators arranged in series with in the operators relate to the same or different one-way functions. Moreover, there is nothing in the cited teachings of Schneier that teaches or suggests means for letting an input to operators be data for verification data generation and an output from the serial sequence of operators be the verification data.

With regard to Claims 8 and 20, the Examiner concludes that Schneier teaches transmitting a public key from a sender to a receiver to allow secure communications.

Applicants respectfully assert that the present claims require much more than the sending of a public key. Applicants content that Schneier does not teach an output means or steps for generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated verification data to its own verification data output section, means or steps for generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated verification data to its own verification data output section, or means or steps for determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually, wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually. Accordingly, the combination of Vainio and Schneier does not obviate the invention as claimed.

The Examiner has rejected Claims 9, 11, 21, 23, 33, 35, 38 and 40 under 35 USC 103(a) as being unpatentable over

Vainio in view of Schneier and further in view of Lin. Applicants again rely on the interpretation set forth above with regard to the teachings of the Vainio and Schneier references. Applicants respectfully assert that, even if one were to modify Vainio with teachings from the additionally cited references, one would not arrive at the invention as claimed. Since none of the cited references teaches or suggests means and steps for generating a plurality of verification data with first generation algorithms, for comparing the plurality of verification data, for defining functions and sequencing operators, for applying second generation algorithms, it cannot be maintained that the combination of references obviates the invention as claimed. Adding the Lin teachings that "computing power, memory capacity and supply power of the portable device may not be sufficient for key generation" (page 12 of Office Action) would not teach or suggest a proposed solution to that insufficiency. Applicants respectfully request reconsideration of the rejections.

The Examiner has rejected Claims 103, 8, 13-15, 20, and 25-27 under 35 USC 103(a) as being unpatentable over Vainio in view of the newly-cited Hind patent. Applicants again rely on the arguments set forth above with respect to the

teachings of the Vainio reference. The Hind patent is cited for teaching the sending of a certificate from one device to another device. As stated by the Examiner, at the Hind device an "identifier of a sending device is displayed and verified". However, the present invention does not teach or suggest displaying and verifying a device identifier. The pending application teaches and claims more than generating verification data with a first generation algorithm. Further, the Examiner states that Hind teaches that verification data is in visual and auditory form. As noted above with respect to the Kuwamoto reference, outputting verification data in user-detectable manners does not obviate the claimed generating of verification data by two different devices, outputting the verification data to first and second verification data output sections, and comparing the data at each of the devices. Clearly, the Hind patent does not provide those teachings which are missing from the Vainio reference. As such, Applicants conclude that *prima facie* obviousness has not been established.
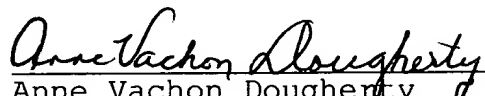
Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

T. Noguchi, et al

By: *Anne Vachon Dougherty*
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910